UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,367	01/31/2002	Robert David Zobel	05456.105009	2476

7590 03/22/2007

Robert T. Neufeld, Esq.
KING & SPALDING
45th Floor
191 Peachtree Street, N.E.
Atlanta, GA 30303

EXAMINER	
SHAW, YIN CHEN	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/066,367	ZOBEL ET AL.	
	Examiner	Art Unit	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/08/2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-9,11-13,15-17,19-27,29-36 and 38-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-5 and 7-11* is/are allowed.

6)☒ Claim(s) *12,13,15-17,19-27,29-36 and 38-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This written action is responding to the Appeal Brief filed on 12/08/2006.
   a. In view of the Appeal Brief file on 12/08/2006, PROSECUTION IS HEREBY RESPONDED. A new ground of rejection is set forth below.
   b. To avoid abandonment of the application, Appellant must exercises one of the following two options:
      i. File a rely under 37 CFR 1.111 (if this Office Action is non-final) or a reply under 37 CFR 1.113 (if this Office Action is final); or,
      ii. request reinstatement of the appeal.

      If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131, 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).
2. Claims 12-13, 15-17, 19-27, 29-36, and 38-45 have been examined and rejected.

Priority

3. The application has been filed under Title 35 U.S.C. 119(e), claiming priority to provisional application 60/265,519, filed on Jan. 31, 2001.
4. The effective filing data for the subject matter defined in the pending claims in this application is Jan. 31, 2001.

Claim Objection

5. Claim 7 is objected to because of the following informalities:

   a. Claim 7 depended on a cancelled claim 6. For examination purpose, Claim 7 is treated as depending on Claim 1.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 12, 21, 38 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

   a. Claims 12, 31, and 38 are directed to non-statutory subject matter since they only recite computer-readable medium with instructions, but without directing to any interaction between physical or technological entity and the medium itself.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 13, 15, 17, 20-26, 29-35, 38-40, 42-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent 6,324,656) and further in view of Proctor (U.S. Patent 6,530,024), and Yang (U.S. Patent 6,467,002).

a. *Referring to Claim 13:*

As per Claim 13, Gleichauf et al. disclose a computer-implemented method for configuring and scheduling a security audit of a computer network comprising the steps of:

conducting a discovery scan to identify an element of the computer network **[An initial phase of the assessment can be a discovery phase. NVA engine 20 is operable to ping devices coupled to network backbone 14 in order to identify all such devices or systems that are so coupled. Such an operation can be called "host discovery." (lines 15-19, Col. 4 from Gleichauf et al.). NVA engine 20 can identify the device type 70 of each device or system coupled to internal network (lines 34-36, Col. 5 from Gleichauf et al.)]**;

configuring an audit scan to perform on the element **[Another phase of the assessment can be a data collection phase. NVA engine 20 can, for example, perform port scans on each device coupled to network backbone 14. NVA engine 20 can further receive banners from the scanned ports. For example, NVA engine 20 could open a**

connection to a port on workstation 12 and receive a telnet banner from that port of workstation 12. NVA engine 20 can use such banner information to create and to maintain port database 22 (lines 20-28, Col. 4 from Gleichauf et al.)].

Gleichauf et al. do not expressly disclose the remaining limitations of the claim. However, Proctor discloses calculating a security score (i.e., assessment result) for the element based on the audit scan by summing one or more vulnerabilities (i.e., threshold or limit range values) associated with the element **[In one embodiment, the detection policy is used to establish thresholds or limits which, when reached, trigger an alarm or other condition indicating that a security breach, attempted security breach, or other network security condition has occurred or is occurring (line 67, Col. 9 and lines 1-4, Col. 10). The security policy can include security settings or values, which define the security of the system (lines 12-13, Col. 10). A detection engine 1342 evaluates the collected events and activities to determine whether a security occurrence exists. For example, as described above, this can include monitoring activities to determine whether established threshold levels have been met or exceeded, whether activities are occurring out of nominal ranges, or whether unauthorized activities are attempted or performed (lines 41-45, Col. 14). The collected records are**

provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908. The security assessment is performed in accordance with the detection policy or policies 916 established for the network, or for that user or workstation (lines 41-48, Col. 11 from Proctor)];

scheduling a time to perform the audit scan (i.e. audit scan that will end collecting for audit data) on the element **[For example, the administrator may choose to collect the audit data from all systems twice daily, once at 4 PM and once at 12 noon. The administrator may identify a different collection schedule for each day, or may identify different schedules for weekdays and weekends. In one embodiment, the administrator can click on a box 712 to select that box 712 as a collection time for that day. Alternatively, the administrator can double click on a time to select every day at that time, or double click on a day to select every time for that day. Additionally, the user can click and drag the pointer across several squares 712 to toggle a group or block of squares on or off. Regardless of the tool provided or screen layout used to select collection days and times, the collection policy establishes when the audited data is to be collected by the security system. As**

would be apparent to one of ordinary skill in the art after reading this description, alternative collection techniques can be employed to allow collection of audit data at desired times or intervals (lines 46-65, Col. 9 from Proctor)]. Yang further discloses assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network **[i.e., Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10 from Yang)]**. Gleichauf et al., Proctor, and Yang are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Gleichauf et al. with a scanning system capable of providing scheduling and vulnerability value assessment value functionality from Proctor and the priority value associated with the devices in the network environment from Yang since one would have been motivated to (1) have a system and method for adapting security procedures based on computing environment activity (lines 7-9, Col. 1 from Proctor) and different audits associated with the procedures and (2) realize that an efficient mechanism for priority arbitration is much needed

in such a shared-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1 from Yang). Therefore, it would have been obvious to modify Gleichauf et al. with Proctor and Yang to obtain the invention as specified in Claim 13.

b. *Referring to Claim 15:*

As per Claim 15, the rejection of Claim 13 is incorporated. In addition, Proctor discloses the step of scheduling another time to perform the audit scan on the element **[Additionally, the user can click and drag the pointer across several squares 712 to toggle a group or block of squares on or off. Regardless of the tool provided or screen layout used to select collection days and times, the collection policy establishes when the audited data is to be collected by the security system. As would be apparent to one of ordinary skill in the art after reading this description, alternative collection techniques can be employed to allow collection of audit data at desired times or intervals (lines 46-65, Col. 9 from Proctor)]**.

c. *Referring to Claim 17:*

As per Claim 17, the rejection of Claim 13 is incorporated. In addition, Gleichauf et al. disclose wherein the step of conducting a discovery scan further comprises identifying at least one of the functions or the one or more vulnerabilities associated with the element **[i.e., According to the**

present invention, NVA engine 20 is operable to perform network vulnerability assessment. In general, this assessment is "multi-phase" in that it can be carried out in multiple steps or phases (lines 9-12, Col. 4). An initial phase of the assessment can be a discovery phase. NVA engine 20 is operable to ping devices coupled to network backbone 14 in order to identify all such devices or systems that are so coupled. Such an operation can be called "host discovery." (lines 15-19, Col. 4). For example, in the embodiment of FIG. 2, NVA engine 20 can identify the device type 70 of each device or system coupled to internal network 10 (lines 33-36, Col. 5). The potential vulnerabilities 80 can also be identified by NVA engine 20. For example, the potential vulnerabilities 80 shown in the embodiment of FIG. 2 can be the potential vulnerabilities inherent to the services 78 and operating system 74 of each device 70 (lines 41-45, Col. 5)].

d. *Referring to Claim 20:*

As per Claim 20, the rejection of Claim 13 is incorporated. In addition, In addition, Proctor discloses wherein the step of configuring an audit scan comprises manually selecting the type of audit scan **[i.e., One example implementation of creating an object audit is illustrated n FIG. 5 (lines 18-20, Col. 8), where the type of object audit can be subjected to variety of edition and modification. Although the functionality is**

not illustrated on the screen diagram of FIG. 5, the functionality can be provided in one embodiment to allow the administrator to create and edit custom groups (lines 50-53, Col. 8). FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9). Additionally, the administrator can select whether to replace auditing on existing sub keys as illustrated by selection box 614 (lines 16-18, Col 9)].

e. *Referring to Claim 21:*

As per Claim 21, Gleichauf et al., Proctor, and Yang disclose the steps recited in claim 13. In addition, Proctor discloses a computer-readable medium having computer-executable instructions **[i.e., FIG. 15 is a block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17)]**.

f. *Referring to Claim 22:*

As per Claim 22, Gleichauf et al. disclose a method for assessing the security of a network comprising the steps of:

receiving an initial scan identifying a network element and function of the network element **[An initial phase of the assessment can be a discovery phase. NVA engine 20 is operable to ping devices coupled to network backbone 14 in order to identify all such devices or systems that are so coupled. Such an operation can be called "host discovery." (lines 15-19, Col. 4 from Gleichauf et al.). NVA engine 20 can identify the device type 70 of each device or system coupled to internal network (lines 34-36, Col. 5 from Gleichauf et al.)]**;

an audit scan to perform on the network element; said audit scan is based on the initial scan; performing the audit scan on the network; receiving data from the audit scan of the network element **[According to the present invention, NVA engine 20 is operable to perform network vulnerability assessment. In general, this assessment is "multi-phase" in that it can be carried out in multiple steps or phases (lines 9-12, Col. 4). Another phase of the assessment can be a data collection phase. NVA engine 20 can, for example, perform port scans on each device coupled to network backbone 14. NVA engine 20 can further receive banners from the scanned ports. For example, NVA engine 20 could open a connection to a port on workstation 12 and receive a telnet banner from that port of workstation 12. NVA engine 20 can use such banner information to**

create and to maintain port database 22 (lines 20-28, Col. 4 from Gleichauf et al.)].

Gleichauf et al. do not expressly disclose the remaining limitations of the claim. However, Proctor discloses selecting processing for the audit scan **[One example implementation of creating an object audit is illustrated in FIG. 5 (lines 18-20, Col. 8 from Proctor). Add, edit and remove buttons 509 can be used to create and modify a list of files to be audited (lines 26-28, Col. 8 from Proctor), *where the audit can be selected and is subjected to variety of edition and modification*]** and calculating a security score (i.e., assessment result) for the element based on the audit scan by summing one or more vulnerabilities (i.e., threshold or limit range values) associated with the element **[In one embodiment, the detection policy is used to establish thresholds or limits which, when reached, trigger an alarm or other condition indicating that a security breach, attempted security breach, or other network security condition has occurred or is occurring (line 67, Col. 9 and lines 1-4, Col. 10). The security policy can include security settings or values, which define the security of the system (lines 12-13, Col. 10). A detection engine 1342 evaluates the collected events and activities to determine whether a security occurrence exists. For example, as described above, this can include monitoring activities to determine whether established**

threshold levels have been met or exceeded, whether activities are occurring out of nominal ranges, or whether unauthorized activities are attempted or performed (lines 41-45, Col. 14). The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908. The security assessment is performed in accordance with the detection policy or policies 916 established for the network, or for that user or workstation (lines 41-48, Col. 11 from Proctor)];

scheduling the audit scan (i.e. audit scan that will end collecting for audit data) to perform on the element; allow the performing of the audit scan on the element at the scheduled time **[For example, the administrator may choose to collect the audit data from all systems twice daily, once at 4 PM and once at 12 noon. The administrator may identify a different collection schedule for each day, or may identify different schedules for weekdays and weekends. In one embodiment, the administrator can click on a box 712 to select that box 712 as a collection time for that day. Alternatively, the administrator can double click on a time to select every day at that time, or double click on a day to select every time for that day. Additionally, the user can click and drag the pointer across several**

squares 712 to toggle a group or block of squares on or off. Regardless of the tool provided or screen layout used to select collection days and times, the collection policy establishes when the audited data is to be collected by the security system. As would be apparent to one of ordinary skill in the art after reading this description, alternative collection techniques can be employed to allow collection of audit data at desired times or intervals (lines 46-65, Col. 9 from Proctor)]. Yang further discloses assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network **[i.e., Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10 from Yang)]**. Gleichauf et al., Proctor, and Yang are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Gleichauf et al. with a scanning system capable of providing scheduling and vulnerability value assessment value functionality from Proctor and the priority value associated with the devices in the network environment from Yang since one would have

been motivated to (1) have a system and method for adapting security procedures based on computing environment activity (lines 7-9, Col. 1 from Proctor) and different audits associated with the procedures and (2) realize that an efficient mechanism for priority arbitration is much needed in such a shared-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1 from Yang). Therefore, it would have been obvious to modify Gleichauf et al. with Proctor and Yang to obtain the invention as specified in Claim 22.

g. *Referring to Claim 23:*

As per Claim 23, the rejection of Claim 22 is incorporated. In addition, Proctor discloses modifying the selected audit scan, said modification based on the data received from the selected audit scan **[i.e., The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908 (lines 41-45, Col. 11). When security assessment 924 determines that an actual attempted or potential security breach has occurred or is occurring, one or more policy updates 928 are made to on or more of the audit policy 904, collection policy 912, and detection policy 916 (lines 49-53, Col. 11)]**.

h. *Referring to Claim 24:*

As per Claim 24, the rejection of Claim 22 is incorporated. Gleichauf et al. further disclose identifying an operating system for the network element **[NVA engine 20 can further identify the operating system 74 of each device and the services 78 available on each device (lines 36-38, Col. 5)]**. In addition, Gleifchauf et al. disclose identifying a service for the network element, the service indicating the element's function; and identifying at lest one vulnerability associated with the network element **[i.e., According to the present invention, NVA engine 20 is operable to perform network vulnerability assessment. In general, this assessment is "multi-phase" in that it can be carried out in multiple steps or phases (lines 9-12, Col. 4). An initial phase of the assessment can be a discovery phase. NVA engine 20 is operable to ping devices coupled to network backbone 14 in order to identify all such devices or systems that are so coupled. Such an operation can be called "host discovery." (lines 15-19, Col. 4). For example, in the embodiment of FIG. 2, NVA engine 20 can identify the device type 70 of each device or system coupled to internal network 10 (lines 33-36, Col. 5). The potential vulnerabilities 80 can also be identified by NVA engine 20. For example, the potential vulnerabilities 80 shown in the embodiment**

of FIG. 2 can be the potential vulnerabilities inherent to the services 78 and operating system 74 of each device 70 (lines 41-45, Col. 5)].

i. *Referring to Claim 25:*

As per Claim 25, it encompasses limitations that are similar to those of Claim 22. Thus, it is rejected with the same rationale applied against Claim 22 above.

j. *Referring to Claim 26:*

As per Claim 26, the rejection of Claim 22 is incorporated. In addition, Proctor discloses wherein the step of selecting an audit scan is based on a manual input **[i.e., One example implementation of creating an object audit is illustrated n FIG. 5 (lines 18-20, Col. 8 from Proctor), *where the type of object audit is subjected to edition and modification*. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9 from Proctor)]**.

k. *Referring to Claim 29:*

As per Claim 29, Gleichauf et al., Proctor, and Yang disclose the steps recited in claim 22. In addition, Proctor discloses a computer-readable medium having computer-executable instructions **[i.e., FIG. 15 is a**

block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17)].

l. *Referring to Claim 30:*

As per Claim 30, Proctor discloses a method for assessing the security of a network comprising the steps of:

receiving an initial scan identifying a network element **[An initial phase of the assessment can be a discovery phase. NVA engine 20 is operable to ping devices coupled to network backbone 14 in order to identify all such devices or systems that are so coupled. Such an operation can be called "host discovery." (lines 15-19, Col. 4 from Gleichauf et al.)]**;

an audit scan to perform on the network element, said audit scan is based on the initial scan; performing the audit scan on the network; receiving data from the audit scan of the network element **[According to the present invention, NVA engine 20 is operable to perform network vulnerability assessment. In general, this assessment is "multi-phase" in that it can be carried out in multiple steps or phases (lines 9-12, Col. 4). Another phase of the assessment can be a data collection phase. NVA engine 20 can, for example, perform port scans on each device coupled to network backbone**

14. NVA engine 20 can further receive banners from the scanned ports. For example, NVA engine 20 could open a connection to a port on workstation 12 and receive a telnet banner from that port of workstation 12. NVA engine 20 can use such banner information to create and to maintain port database 22 (lines 20-28, Col. 4 from Gleichauf et al.)]. Gleichauf et al. do not expressly disclose the remaining limitations of the claim. However, Proctor discloses selecting processing for the audit scan **[One example implementation of creating an object audit is illustrated in FIG. 5 (lines 18-20, Col. 8 from Proctor). Add, edit and remove buttons 509 can be used to create and modify a list of files to be audited (lines 26-28, Col. 8 from Proctor),** ***where the audit can be selected and is subjected to variety of edition and modification***] and calculating a security score (i.e., assessment result) for the element based on the audit scan by summing one or more vulnerabilities (i.e., threshold or limit range values) associated with the element **[In one embodiment, the detection policy is used to establish thresholds or limits which, when reached, trigger an alarm or other condition indicating that a security breach, attempted security breach, or other network security condition has occurred or is occurring (line 67, Col. 9 and lines 1-4, Col. 10). The security policy can include security settings or values, which define the security of the system (lines 12-13, Col.**

10). A detection engine 1342 evaluates the collected events and activities to determine whether a security occurrence exists. For example, as described above, this can include monitoring activities to determine whether established threshold levels have been met or exceeded, whether activities are occurring out of nominal ranges, or whether unauthorized activities are attempted or performed (lines 41-45, Col. 14). The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908. The security assessment is performed in accordance with the detection policy or policies 916 established for the network, or for that user or workstation (lines 41-48, Col. 11 from Proctor)]. Yang further discloses assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network **[i.e., Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10 from Yang)]**. Gleichauf et al., Proctor, and Yang are analogous art because

they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Gleichauf et al. with a scanning system capable of providing scheduling and vulnerability value assessment value functionality from Proctor and the priority value associated with the devices in the network environment from Yang since one would have been motivated to (1) have a system and method for adapting security procedures based on computing environment activity (lines 7-9, Col. 1 from Proctor) and different audits associated with the procedures and (2) realize that an efficient mechanism for priority arbitration is much needed in such a shared-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1 from Yang). Therefore, it would have been obvious to modify Gleichauf et al. with Proctor and Yang to obtain the invention as specified in Claim 30.

m. *Referring to Claim 31:*

As per Claim 31, Gleichauf et al., Proctor, and Yang disclose the method of claim 30, further comprising the step of scheduling the selected audit scan, said scheduling based on the initial scan **[[Regardless of the tool provided or screen layout used to select collection days and times, the collection policy establishes when the audited data is to be collected by the security system. As would be apparent to one of**

ordinary skill in the art after reading this description, alternative collection techniques can be employed to allow collection of audit data at desired times or intervals (lines 46-65, Col. 9 from Proctor)] and [According to the present invention, NVA engine 20 is operable to perform network vulnerability assessment. In general, this assessment is "multi-phase" in that it can be carried out in multiple steps or phases (lines 9-12, Col. 4 from Gleichauf et al.). An initial phase of the assessment can be a discovery phase. NVA engine 20 is operable to ping devices coupled to network backbone 14 in order to identify all such devices or systems that are so coupled. Such an operation can be called "host discovery." (lines 15-19, Col. 4 from Gleichauf et al.)]].

n. *Referring to Claim 32:*

As per Claim 32, Gleichauf et al., Proctor, and Yang disclose the method of claim 30. In addition, Proctor discloses modifying the selected audit scan, said modification based on the data received from the selected audit scan **[i.e., The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908 (lines 41-45, Col. 11). When security assessment 924 determines that an actual attempted or potential**

security breach has occurred or is occurring, one or more policy updates 928 are made to on or more of the audit policy 904, collection policy 912, and detection policy 916 (lines 49-53, Col. 11)].

o. *Referring to Claim 33:*

As per Claim 33, Gleichauf et al., Proctor, and Yang disclose the method of claim 30. In addition, Gleichauf et al. disclose wherein the step of receiving an initial scan comprises:

identifying an operating system and a service for the network element, and identifying at least one vulnerability associated with the network element **[i.e., NVA engine 20 can further identify the operating system 74 of each device and the services 78 available on each device (lines 36-38, Col. 5). The potential vulnerabilities 80 can also be identified by NVA engine 20. For example, the potential vulnerabilities 80 shown in the embodiment of FIG. 2 can be the potential vulnerabilities inherent to the services 78 and operating system 74 of each device 70 (lines 41-45, Col. 5 from Gleichauf et al.)]**.

p. *Referring to Claim 34:*

As per Claim 34, it encompasses limitations that are similar to those of Claim 30. Thus, it is rejected with the same rationale applied against Claim 30 above.

q. *Referring to Claim 35:*

As per Claim 35, Gleichauf et al., Proctor, and Yang disclose the method of claim 30, wherein the step of selecting an audit scan is based on a manual input **[i.e., One example implementation of creating an object audit is illustrated n FIG. 5 (lines 18-20, Col. 8 from Proctor), *where the type of object audit is subjected to edition and modification.* FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9 from Proctor)]**.

r. *Referring to Claim 38:*

As per Claim 38, Gleichauf et al., Proctor, and Yang disclose the steps recited in claim 30. In addition, Proctor discloses a computer-readable medium having computer-executable instructions **[i.e., FIG. 15 is a block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17)]**.

s. *Referring to Claim 39:*

As per Claim 39, Gleichauf et al. disclose a system for configuring and scheduling a security audit of a computer network comprising:

the computer network **[internal network 10 (line 30, Col. 3 and Fig. 1 from Gleichauf et al.)]**;

a security audit system operable for conducting a discovery scan to identify an element of the computer network **[An initial phase of the assessment can be a discovery phase. NVA engine 20 is operable to ping devices coupled to network backbone 14 in order to identify all such devices or systems that are so coupled. Such an operation can be called "host discovery." (lines 15-19, Col. 4 from Gleichauf et al.). NVA engine 20 can identify the device type 70 of each device or system coupled to internal network (lines 34-36, Col. 5 from Gleichauf et al.)]**;

configuring an audit scan of the element **[Another phase of the assessment can be a data collection phase. NVA engine 20 can, for example, perform port scans on each device coupled to network backbone 14. NVA engine 20 can further receive banners from the scanned ports. For example, NVA engine 20 could open a connection to a port on workstation 12 and receive a telnet banner from that port of workstation 12. NVA engine 20 can use such banner information to create and to maintain port database 22 (lines 20-28, Col. 4 from Gleichauf et al.)]**.

Gleichauf et al. do not expressly disclose the remaining limitations of the claim. However, Proctor discloses computing a security score (i.e., assessment result) for the network element from the selected audit scan by summing one or more vulnerabilities (i.e., threshold or limit range values) associated with the network element **[In one embodiment, the detection policy is used to establish thresholds or limits which, when reached, trigger an alarm or other condition indicating that a security breach, attempted security breach, or other network security condition has occurred or is occurring (line 67, Col. 9 and lines 1-4, Col. 10). The security policy can include security settings or values, which define the security of the system (lines 12-13, Col. 10). A detection engine 1342 evaluates the collected events and activities to determine whether a security occurrence exists. For example, as described above, this can include monitoring activities to determine whether established threshold levels have been met or exceeded, whether activities are occurring out of nominal ranges, or whether unauthorized activities are attempted or performed (lines 41-45, Col. 14). The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908. The security**

assessment is performed in accordance with the detection policy or policies 916 established for the network, or for that user or workstation (lines 41-48, Col. 11 from Proctor)];

scheduling the audit scan (i.e. audit scan that will end collecting for audit data) on the element **[For example, the administrator may choose to collect the audit data from all systems twice daily, once at 4 PM and once at 12 noon. The administrator may identify a different collection schedule for each day, or may identify different schedules for weekdays and weekends. In one embodiment, the administrator can click on a box 712 to select that box 712 as a collection time for that day. Alternatively, the administrator can double click on a time to select every day at that time, or double click on a day to select every time for that day. Additionally, the user can click and drag the pointer across several squares 712 to toggle a group or block of squares on or off. Regardless of the tool provided or screen layout used to select collection days and times, the collection policy establishes when the audited data is to be collected by the security system. As would be apparent to one of ordinary skill in the art after reading this description, alternative collection techniques can be employed to allow collection of audit data at desired times or intervals (lines 46-65, Col. 9 from Proctor)]**.

Proctor further discloses a console operable for receiving and

transmitting information about the audit scan **[i.e., Security procedures can also be applied to security console 104B (lines 42-43, Col. 5). In one embodiment, the security procedures can include for example, one or more of security policies, collection policies, detection policies and audit policies. The security console 104B can also perform the adaptive feedback operations, including updating the security procedures based on security occurrences (lines 45-47, Col. 5). The example embodiment illustrated in FIG. 3, the audit policy 300 includes a system audit 304, and object audit 324, and a registry key audit 334 (lines 48-50, Col. 7)]**. Yang further discloses assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network **[i.e., Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10 from Yang)]**. Gleichauf et al., Proctor, and Yang are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Gleichauf et al. with a scanning system capable of providing scheduling

and vulnerability value assessment value functionality from Proctor and the priority value associated with the devices in the network environment from Yang since one would have been motivated to (1) have a system and method for adapting security procedures based on computing environment activity (lines 7-9, Col. 1 from Proctor) and different audits associated with the procedures and (2) realize that an efficient mechanism for priority arbitration is much needed in such a shared-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1 from Yang). Therefore, it would have been obvious to modify Gleichauf et al. with Proctor and Yang to obtain the invention as specified in Claim 39.

t. *Referring to Claim 40:*

As per Claim 40, the rejection of Claim 39 is incorporated. In addition, Gleichauf et al. disclose wherein the security audit system is further operable for conducting a discovery scan to:

Identifying a function for the element; and identifying at least one vulnerability for the element **[i.e., According to the present invention, NVA engine 20 is operable to perform network vulnerability assessment. In general, this assessment is "multi-phase" in that it can be carried out in multiple steps or phases (lines 9-12, Col. 4). An initial phase of the assessment can be a discovery phase. NVA engine 20 is operable to ping devices coupled to network backbone**

14 in order to identify all such devices or systems that are so coupled. Such an operation can be called "host discovery." (lines 15-19, Col. 4). For example, in the embodiment of FIG. 2, NVA engine 20 can identify the device type 70 of each device or system coupled to internal network 10 (lines 33-36, Col. 5). The potential vulnerabilities 80 can also be identified by NVA engine 20. For example, the potential vulnerabilities 80 shown in the embodiment of FIG. 2 can be the potential vulnerabilities inherent to the services 78 and operating system 74 of each device 70 (lines 41-45, Col. 5)].

u. *Referring to Claim 42:*

As per Claim 42, Gleichauf et al., Proctor, and Yang disclose the system of claim 39. In addition, Gleichauf et al. disclose wherein the security audit system further comprises a system scanning engine operable for detecting particular one of the vulnerabilities on the network element **[i.e., Similar to FIG. 1, NVA engine 20 is coupled to network backbone 14 and is coupled to and in communication with port database 22, rule set 24, and datamine database 26. In operation, NVA engine 20 is operable to perform a network vulnerability assessment of internal network 10 (lines 24-26, Col. 5). The potential vulnerabilities 80 can also be identified by NVA engine 20. For example, the potential vulnerabilities 80 shown in the embodiment of FIG. 2 can be the potential vulnerabilities inherent**

to the services 78 and operating system 74 of each device 70 (lines 41-45, Col. 5 from Gleichauf et al.)].

v. *Referring to Claim 43:*

As per Claim 43, Gleichauf et al., Proctor, and Yang disclose the system of claim 39. In addition, Gleichauf et al. disclose wherein the security audit system further comprises an Internet scanning engine operable for performing a discovery scan on the network **[i.e., In operation, NVA engine 20 is operable to perform a network vulnerability assessment of internal network 10. The assessment can include, as discussed with respect to FIG. 1, a discovery phase and data collection phase. By executing such processes, NVA engine 20 can identify the configuration of internal network 10 and uncover the various dimensions within internal network 10 (lines 27-33, Col. 5 from Gleichauf et al.)]**.

w. *Referring to Claim 44:*

As per Claim 44, Gleichauf et al., Proctor, and Yang disclose the system of claim 39, wherein the security audit system further comprises a database scanning engine operable for detecting vulnerabilities associated with database elements within the network **[NVA engine 20 can create datamine database 26 from the resulting data, and datamine database 26 can include potential vulnerabilities in internal network 10. NVA engine 20 can further perform active**

exploits on network 10 to confirm the identified potential vulnerabilities (lines 52-57, Col. 5 from Gleichauf et al.)].

x. *Referring to Claim 45:*

As per Claim 44, Gleichauf et al., Proctor, and Yang disclose the system of claim 39, wherein the security audit system further comprises an active scan engine operable for selecting coordinating, and scheduling various discovery and audit scans to be performed on the computer network **[In operation, NVA engine 20 is operable to perform a network vulnerability assessment of internal network 10. The assessment can include, as discussed with respect to FIG. 1, a discovery phase and data collection phase. By executing such processes, NVA engine 20 can identify the configuration of internal network 10 and uncover the various dimensions within internal network 10. For example, in the embodiment of FIG. 2, NVA engine 20 can identify the device type 70 of each device or system coupled to internal network 10. NVA engine 20 can further identify the operating system 74 of each device and the services 78 available on each device. Such data can be incorporated into port database 22, for example, as entries populating fields of port database 22 (lines 27-40, Col. 5 from Gleichauf et al.) and Regardless of the tool provided or screen layout used to select collection days and times, the collection policy establishes when the audited data is to be**

collected by the security system. As would be apparent to one of ordinary skill in the art after reading this description, alternative collection techniques can be employed to allow collection of audit data at desired times or intervals (lines 59-65, Col. 9 and Fig. 7 from Proctor)].

8. Claims 16, 27, 36, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent 6,324,656), Proctor (U.S. Patent 6,530,024), and Yang (U.S. Patent 6,467,002) as applied to claims 1, 13, 22, and 39 above, and further in view of Hartley et al. (U.S. Patent 6,889,168).

   a. *Referring to Claim 16:*

      As per Claim 16, Gleichauf et al., Proctor, and Yang disclose the method of claim 3. Proctor, Gleichauf et al., Kingsford et al., Hartley et al. and Yang do not explicitly disclose the step of receiving a blackout time during which no audit scan can be scheduled. However, Hartley et al. disclose scheduling module which is used for specifying the time of conducting security modules or all the test based on the specific time availability (i.e., free period, blackout period, et ...) **[i.e., The schedule module 32 provides the functionality to run security checks at predetermined intervals. Checks can be scheduled to run at specific designated times as well as at regular intervals such as monthly or weekly. The schedule module further provides the**

flexibility to run individual security modules or all tests (lines 9-14, Col. 7). A variety of further screens may be presented which provide the system user the choices of one or more modules scheduled, the data which the function will be performed. Further options may be provided such as periodic activation of the functions, one time activations of the functions, or the combination of various security and utility modules (lines31-38, Col. 10)]. Gleichauf et al., Proctor, Yang, and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Gleichauf et al., Proctor, and Yang with the scheduling module that can provide flexibility in the scheduling of the scanning from Hartley et al. since one would have been motivated to have the schedule module for providing the flexibility to run individual security modules or all tests (lines 12-14, Col. 7 from Hartley et al.). Therefore, it would have been obvious to modify Gleichauf et al., Proctor, and Yang with Hartley et al. to obtain the invention as specified in Claim 16.

b. *Referring to Claim 27:*

As per Claim 27, the rejection of Claim 22 is incorporated. In addition, Claim 27 encompasses limitations that are similar to those of Claim 16.

Thus, it is rejected with the same rationale applied against Claim 16 above.

c. *Referring to Claim 36:*

As per Claim 36, the rejection of Claim 30 is incorporated. In addition, Claim 36 encompasses limitations that are similar to those of Claim 16. Thus, it is rejected with the same rationale applied against Claim 16 above.

d. *Referring to Claim 41:*

As per Claim 41, the rejection of Claim 39 is incorporated. In addition, Claim 41 encompasses limitations that are similar to those of Claim 16. Thus, it is rejected with the same rationale applied against Claim 16 above.

9. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over, Gleichauf et al. (U.S. Patent 6,324,656), Proctor (U.S. Patent 6,530,024), and Yang (U.S. Patent 6,467,002) as applied to claims 13 above, and further in view of and Barroux (U.S. Patent 6,220,768).

a. *Referring to Claim 19:*

As per Claim 19, Gleichauf et al., Proctor, and Yang disclose the method of claim 13, wherein the step of configuring an audit scan comprising: retrieving an asset value based on the discovering scan **[[assigns an initial priority order to the plurality of devices such tat those**

devices have priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10 from Yang)] and [i.e., In operation, NVA engine 20 is operable to perform a network vulnerability assessment of internal network 10. The assessment can include, as discussed with respect to FIG. 1, a discovery phase and data collection phase. By executing such processes, NVA engine 20 can identify the configuration of internal network 10 and uncover the various dimensions within internal network 10 (lines 27-33, Col. 5 from Gleichauf et al.)]];

assigning a role and a policy based on the discovery scan **[In operation, NVA engine 20 is operable to perform a network vulnerability assessment of internal network 10. The assessment can include, as discussed with respect to FIG. 1, a discovery phase and data collection phase. By executing such processes, NVA engine 20 can identify the configuration of internal network 10 and uncover the various dimensions within internal network 10. For example, in the embodiment of FIG. 2, NVA engine 20 can identify the device type 70 of each device or system coupled to internal network (lines 27-33, Col. 5 from Gleichauf et al.). NVA engine 20 can apply rule set 24 to port database 22. As discussed with respect to FIG 1, such a process can be an analysis phase of the network**

vulnerability assessment (lines 46-49, Col. 5 from Gleichauf et al.)]. Gleichauf et al., Proctor, and Yang do not expressly disclose retrieving a scan frequency associated with the asset value. Barroux discloses retrieving an scan frequency by scheduling of tasks required for repetition **[Integrated resource 200 also computes whether tasks need to be repeated and builds an interval schedule for tasks requiring repetition into its schedule (lines 36-38, Col. 4)]**. Gleichauf et al., Proctor, Yang, and Barroux are analogous art because they are from similar technology relating to the computer system in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Gleichauf et al., Proctor, Yang, with Barroux to have the priority values associated to the network elements converted into repetitively scheduled tasks since one would have been motivated to collect survey information for a TCP/IP network to develop from the extracted information an asset database characterizing a current configuration of asset at the nodes (lines 10-12 and 30-32, Col. 2 from Barroux). Therefore, it would have been obvious to modify Gleichauf et al., Proctor, and Yang with Barroux to obtain the invention as specified in Claim 19.

Allowable Subject Matter

10. Claim 1-5 and 8-11 are allowed. Claim 1 is allowed because the recited limitation on scheduling another time to repeat the audit scan based on the results of the audit scan and the security score. None of the cited references discussed about scheduling another time to repeat the audit scan based on the results of the audit scan and the security score.
11. Claim 7 is allowable if it overcomes the objection for improper dependency.
12. Claim 12 is allowable if it overcomes the rejection under 35 USC 101.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
    a. Fox et al. (U.S. Patent 6,883,101) disclose a method and data processing system assesses the security vulnerability of a network. A system object model database is created and supports the information data requirements of disparate network vulnerability analysis programs. Only the required data from the system object model database representing the network is imported to the programs, which then analyze the network to produce data results from each program. These data results are stored in a common system model database and within the data fact base. Goal oriented fuzzy logic decision rules are applied to determine the vulnerability posture of the network.

b. Swiler et al. (U.S. Patent 7,013,395) disclose a computer system analysis tool and method that will allow for qualitative and quantitative assessment of security attributes and vulnerabilities in systems including computer networks. The invention is based on generation of attack graphs wherein each node represents a possible attack state and each edge represents a change in state caused by a single action taken by an attacker or unwitting assistant. Edges are weighted using metrics such as attacker effort, likelihood of attack success, or time to succeed. Generation of an attack graph is accomplished by matching information about attack requirements (specified in "attack templates") to information about computer system configuration (contained in a configuration file that can be updated to reflect system changes occurring during the course of an attack) and assumed attacker capabilities (reflected in "attacker profiles"). High risk attack paths, which correspond to those considered suited to application of attack countermeasures given limited resources for applying countermeasures, are identified by finding "epsilon optimal paths."

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F. If

attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Mar. 19, 2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100